Asian Journal of Information Technology 6 (8): 847-853, 2007
ISSN: 1682-3915

A Specification of an Application Gateway for Client/Server Systems

A.J. Jegede, G.I.O. Aimufua and H.O. Salami
Department of Mathematical Sciences,
Nasarawa State University, Keffi, Nigeria

Abstract: The goal of this study is to develop a model of an application gateway that can be used to manage perimeter security in a client/server environment. The gateway acts as a traffic controller between the internal (client/server) LAN and external networks and systems. It ensures that only authorized packets are allowed to go into the LAN from the external systems. It also, guarantees that unauthorized packets are not forwarded to the external environment from the internal local area network. The research conducts an exploratory study of computer networks and client/server systems as well as some of the dangers posed to computer networks. It also examines some of the attempts at curbing network related security threats as well as the strengths and weaknesses of each approach. The study concludes by formulating a model of an application gateway for managing security in client/server environments. The system design tools used in this study is basically the data flow diagram. Possible areas of future study include the extension of the model to support more protocols; the exploration of the need to combine the benefits of the traditional packet filtering processes with those of an application gateway as well as the possibility of integrating the model with other network security strategies.

Key words: Application gateway, client/server systems, communication protocols, network communication, security, traffic-controller

INTRODUCTION

Computer networks have become increasing popular since the emergence of the ARPANET in the 1960s. A communication network can be defined as the interconnection of various computer systems and auxiliary devices (Poulsen, 1999). In other words, a network is a set of equipment and facilities that provides a service: The transfer of information between users located at various geographical locations (Leon and Widjaja, 2000). A network is thus a way to connect computers so that they can communicate, exchange information and pool resources (Norton, 1996).

The increasing popularity of communication (or computer) networks is largely due to their inability to provide an almost instantaneous transfer of information from one geographical point to another. This was the view of Leon and Widjaja (2000) when he made this assertion: "The ability of communications at extremely high speed allows users to gather information in large volumes nearly instantaneously and with the aid of computers to almost immediately exercise action at a distance." These unique capabilities form the basis for many existing services and an unlimited number of future based systems.

Some of the benefits of connecting computers in a network include:

Resource sharing: Interconnecting computers facilitates the sharing of hardware resources such as hard disks, scanners and printers and software resources such as program and data files. Access to these resources take place via the communication links between the connected systems.

Ease of communication: Since the systems are connected via communicable links, it is easy for a user to send and receive information to and from other users on the network.

Distributed processing: Any job that would have been handled by just a system can be broken down into smaller chunks, with each chunk assigned to a system on the network. The results are then pooled together after all the systems have completed the tasks assigned to them to form the solution to the original problem. This facilitates higher throughput and less turnaround time.

Fault tolerance: Computer networks facilitates fault tolerance by providing a way to configure the network in such a way that tasks which cannot be completed by any of the interconnected systems due to one form of failure or the other can be easily be taken over by another system. This guarantees reliability and fail-safe.

Corresponding Author: A.J. Jegede, Department of Mathematical Sciences, University of Nasarawa State, Keffi, Nigeria

Client/server systems: A client/server environment consists of two major types of systems: the server and the clients. The server is bigger and faster than the clients. It also possesses a larger internal storage capacity. In a client/server environment, dedicated servers share resources and provide security while the client computers access the shared resources. The client/server architecture is a very popular computing approach because of its advantages over other approaches. These advantages according to Poulsen (1999) include:

- Support for many users
- Centralized administration of shared resources; that is, client/server systems provide a secured and controlled environment in which shared resources can be located and supported.
- Centralized data storage: They enable critical data to be backed up easily.
- Centralized security administration: They allow consistent security policies to be applied to each user on the network.

In a client/server environment, every form of communication-internal and external-goes through the server. For example, if a client A wants to request a service from another client B, it will first forward its request to the server. The server will then forward this request to B. B's response to A will also first be forwarded to the server and then to A.

Even if a client system requests a service from an external network such as the Internet, the request must first go through the server. The server then forwards the request to the intended destination. The service from the destination will also have to pass through the server before it reaches the client who actually requested for the service.

In spite of the appealing benefit of communication network (particularly client/server system), a lot of dangers are still being passed to these system. Anonymous (2001) organized these threats into three broad categories:

Eternal attack: These attacks are those that originate from the internet or from system beyond the access device. External attacks can come in form of web page defacements, virus, Trojan program (also known as Trojan horse) and denial of service by malicious systems crackers and cyber- terrorist. Protection against eternal attacks can be achieved by the use of firewall, network-monitoring devices, distribution of services across the networks and the establishment of bandwidth by protocol or service.

Internal attacks: Internal attacks are those that originate from within the organisation. They are mainly caused by disgruntled employees, curious users and accidental misuse. To protect against eternal attacks users should only be given access and privileges to accomplish their works. Moreover, examining network data paths and splitting of service across multiple networks and system provides higher security and minimize the effect of attack.

Physical attacks: Physical attacks include simple actions such as unplugging equipment and rearranging cable or physically damaging component. Another aspect of physical attacks is the ability of a user to see and analyze network traffic that travel over the same network more of the use's desktop computer. This is known as electronic eavesdropping. It can be prevented by physically isolation network traffic based on the reeds of a particular system.

APPROACHES TO PROVIDING SECURE NETWORKS

The focus of this study is to examine the various approaches used to protect networks. We shall take a brief look at firewall, Intrusion Detection System (IDS), vulnerability assessment tools (also known as scanners), logging and auditing tools and cryptography.

Firewalls: Anonymous (2001) defined a firewall as "any device used as a network-level control mechanism for a network or a set of networks." Basically, firewalls are used to prevent outsiders from accessing an internal network. They can also be used to create more secure pockets within internal LANS for highly sensitive functions. Firewalls work based on the policy defined to govern the exchange of information within a network or between a group of networks. Curtain lends credence to this fact by defining a firewall as "a system or a group of system that forces an access control policy between two networks". According to Avolio and Ranum (1994), firewalls are designed to serve as a control point to and from a network. The perform this role by evaluating connection request as they are received and checking whether or not the network traffic should be allowed based on the predefined set of rules.

Though firewall technology seems to be effective, it is however, not without some flaws. Hughes (1995) stated that "some studies suggest that the used of firewalls is impractical in environment were users critically depends

on distributed applications". This assertion is true to a large extent, because firewalls can implement strict security policies, which make this environment bogged down. This makes what is gained in security to be lost in functionality. Another serious issue is that of a passive and false sense of security. For example, it is possible for an attacker to break into a network by completely by-passing the firewall if he can find an unscrupulous in finder who can be fooled into giving access to a modem port.

Intrusion Detection System (IDS): Bace (2000) defined intrusion detection as the detection of break-ins or break-in attempt either manually or via software expert systems that operate on logs or other information available on the network a similar view was share by Anonymous (2001) when he defined intrusion detection as "the acts of detecting a hostile user or an intruder who is attempting to gain unauthorized access". Intrusion detection system can therefore, be described as a manual or software expert system that performs the tasks of detecting illegal access to a system or network.

Proctor (2001) classified modem day IDS into two distinct categories: Misuse detection models and anomaly based models. He also identified the two implementation of the misuse detection model. These are Network-based Intrusion Detection System (NIDS) are Host-based Intrusion Detection System (HIDS). NIDS are raw-packet passing Engines which capture network traffic and compare them with a set of known attack pattern or signatures. Host-based IDSs, on the other hand, have component that parse logs and watch loggings and processes in other to detect unauthorized access. The philosophy behind normally-based models is to understand the pattern of users and traffic on the network and find deviations in those patterns.

Some of the short coming of IDS includes the inability to eliminate false positives completely. This calls for a serious concern because false positive can jeopardize the overall effectiveness of the intrusion detection effort. Another limitation is the possibility of an IDS (example a normally-based IDS) to detects that some thing was wrong without knowing that specifically the source of the problem was.

Logging and auditing tools: Logs can be used to troubleshoot problems, to track down network anomalies and to trace an intrusion's steps. The easiest way to create secure logging strategies according to Berkeley (1996) is to write logs to one-way-write-once device or to copy logs to a secure logging server. Forrest *et al.* (1997), however, identify a little more scalable approach which revolves around the syslog protocol. This provides administrators with a way to centralize their logs thus giving security teams a single point in which to coordinate all data logs. In addition to centralizing all logs, using at least one third-party logging or passing tool can help beef up security. Federrath *et al.* (1997) identified two advantages of this approach:

- Few crackers have the knowledge or the means to circumvent third- party logging software.
- Good third party software packages derive their logs independently of the operating systems logs and this makes them difficult to circumvent.

Vulnerability assessment tools (scanners): Vulnerability assessment tools or scanner were developed to automate the process of hunting down the security tools that reside on systems. Anonymous (2001) traced the tools of scanners to Chris (1992) who is created the Internet Security Scanner (1SS), that could be used to remotely probe UNIX systems for a set of common vulnerabilities. The vulnerability data, the scanning mechanism and the reporting mechanism are the most common components found in most scanning approaches. The vulnerability data consist of internal data base of vulnerability information that helps scanners to accurately identify remotely systems exposure points.

Scanners are, however, not without limitations. A review carried out by Herberlein *et al.* (2001) showed that many scanners catch a fairly high number of known vulnerabilities but none is equipped to identify all of them. It was also, identified that most scanners do not have timely updates. Moreover, the products still struggle with false positives. For example, on large and diverse networks, they frequently misfire and report on vulnerability that simply does not exist.

CRYPTOGRAPHY

Cryptography is traditionally associated with maintaining the secrecy of a message when the means of communication or storing that message may be subject to misused by attackers. Longley *et al.* (1992) defined cryptography as a method used to ensure secrecy and-or authenticity of messages Menezes *et al.* (1997) went further to defined cryptography as the study of mathematical techniques relating to aspect of information security such as confidentiality, data integrity, entity, authentication and data origin authentication.

A scientific attribute of cryptography was

emphasized in both Patterson (2004) and Akdeniz (1996). Patterson (2004) defined cryptography as the science or art of secret writing. An enhanced scientific approach to the definition of cryptography was given by Akdeniz (1996) in a study titled "cryptography and encryption" when he defined cryptography as 'the science and study' of secret writing which concerns the ways in which communication and data can encoded to prevent disclosure of their contents through eavesdropping or message interception using code, ciphers and other methods, so that only certain people can see the real message. Aydos (2000) also, share their views by describing cryptography as the science of concealing data. This opinion was further asserted by Rabah (2004) and share by Olorunfemi and Oladipo (2006).

Milenkovic (1992) attributed one of the first known ciphers to Julius Caesar. Caesar's ciphers belong to a more general class of substitution ciphers. According to Baker and Piper (1985) a substitution ciphers operate by replacing each symbol or a group of symbols in a plain text by other symbols in other to disguise the original. The relevance of cryptography to data communication is enhanced by the need for information to be handled by a transmission or storage system which is opened to attack. The strength of cryptography, according to Carroll and Robbin (1988) is based on the following factors:

- The secrecy of the cryptographic algorithm
- The secrecy of the key used
- The mathematical complexity of the algorithm.

Attacks on cryptographic systems may be of a mathematical nature, which takes the algorithm itself, or of a simple devious nature which exploit some weaknesses in the implementation or management of cipher systems (Coppersmith, 1987). If the cipher algorithm is known, the attacker might attempt a key exhaustion (or brute-force) attack by exploiting the computational speed of the computer to search the entire key space in comparatively short period of time (Milenkovic, 1992).

MODELLING THE SYSTEM

The proposed gateway is expected to manage security in a LAN- based client/server environment. The gateway checks the validity of every packet that comes into it by using information such as the source address, destination address, protocol and access right. It then decides whether the packet should be forwarded to the internal destination or not. The efficiency of the checking is ensured by forcing all incoming and outgoing network traffic to go through the gateway. That is, no traffic which by passes the gateway, for example by using moderns, in permitted. The following services are supported y the proposed system:

- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Domain Name system (DNS)
- TELNET

System design: Top- down approach is used in designing the system. Top-down design look at the larger picture of the system and then explode it into smaller parts or subsystems (Kendall and Kendall, 1995). Top-down approach is chosen because it allows ascertaining overall system objective first along with ascertaining how they are best met in the overall system. It provides desirable emphasis on the interfaces that the system or subsystem requires, which is lacking in the bottom-up approach. In addition to this, top-down approach provides the means of avoiding the chaos of attempting to design the system "all at once". Since planning and implementing a system

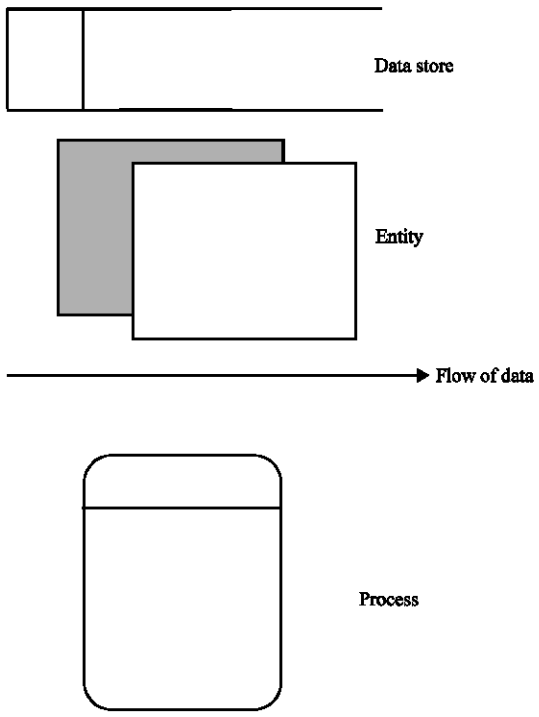

Fig. 1: Data flowing diagram symbols

is a complex process, an attempt to get all subsystems in place and running at once will definitely lead to a failure.

The top-down approach used here decomposes the

entire system into three distinct groups. These three groups are presented here using three different types of diagrams, namely: The context diagram, diagram O and the child diagrams.

The design tool: The design tool used in this study is basically the data flow diagram. Four basic symbols consisting of a double square, an arrow, a rectangle with rounded corners and an open-ended rectangle are used to chart data movements in data flow diagrams. Figure 1 shows the various data flow diagram symbols and their meanings.

The context diagram: The context diagram in Fig. 2 gives an overall picture of the application gateway. It consists of the external network, the application gateway and the local area network. The external and the local area network are treated as entities while the application gateway is regarded as a process.

Fig. 2: The context diagram

Diagram O: Explosion of the context diagram: Diagram O is the result of the decomposition of the context diagram. It gives a breakdown of the various processes involved in the operation of the gateway. Here, the gateway process in Fig. 1 is decomposed into five separate processes, namely: proxy-type determination, DNS proxy, HTTP proxy, FTP proxy and Telnet proxy. This is as shown in Fig. 3.

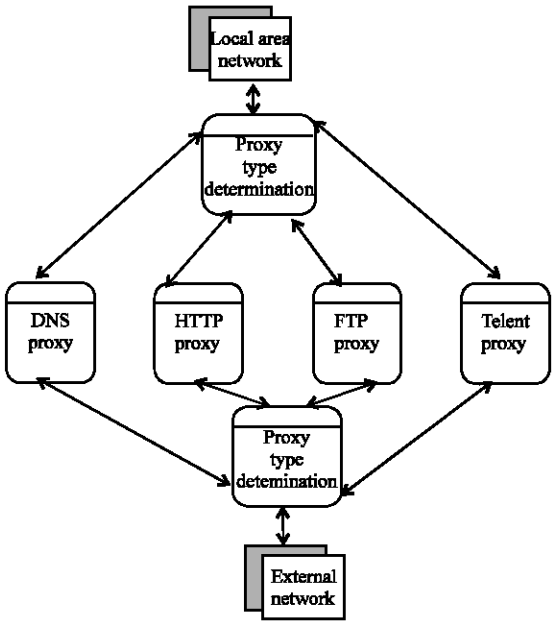

Fig. 3: Explosion of the context diagram

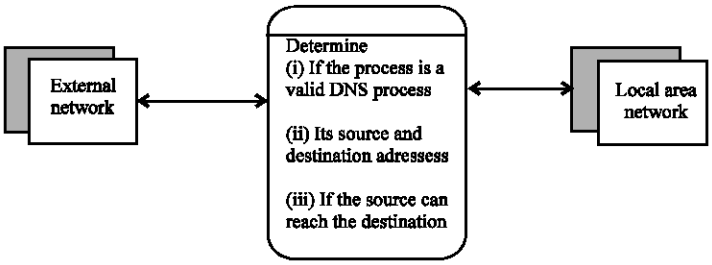

Fig. 4: DNS proxy showing how the gateway handles a DNS process

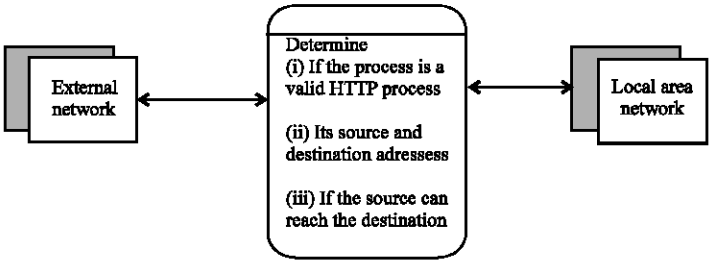

Fig. 5: HTTP proxy showing how the gateway handles an HTTP process

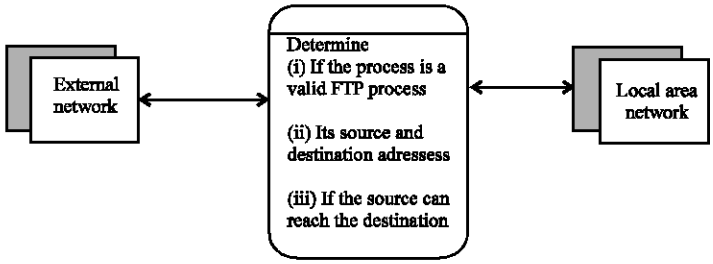

Fig. 6: FTP proxy showing how the gateway handles an FTP process

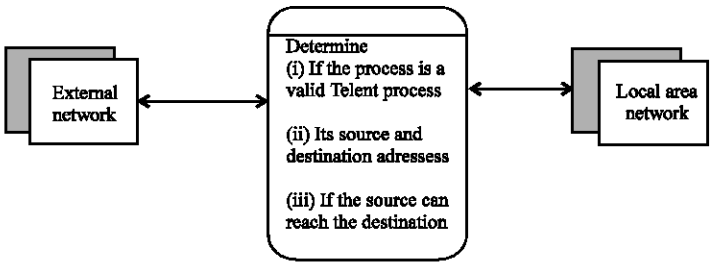

Fig. 7: Telnet proxy showing how the gateway handles a Telnet process

Child diagrams: Further decomposition of diagram O gives rise to four different child diagrams (as shown in Fig. 4-7). These diagrams give a detailed description of the operation of each of the proxy processes in Fig. 4.

CONCLUSION

This study proposes a model of an application gateway that can be used to manage perimeter security in a client/server environment. The gateway stands between a local area network (connected in a client/server mode) and the external networks and systems. It ensures that only authorized packets are allowed to enter or leave the internal LAN. The model of a gateway proposed here will be implemented in a future work as a totally decentralized distributed application consisting of three main subsystems: Generate packet system, AppGateway system and Learning system. These subsystems will work together to achieve the overall objectives of the gateway system. Java is the proposed language of implementation because it is very suitable for network communications and it has extensive routines for dealing with communication protocols. The existence of these routines provides Java with the capability and the flexibility to communicate with TCP/IP protocol such as HTTP, FTP, etc.

Possible areas of future study includes the extension of the model to support more protocols; the need to combine the benefits of traditional packet filtering with those of an application gateway as well as the exploration of the possibility of merging the model with other network security models in order to obtain an enhanced network security suite.

REFERENCES

Anonymous, 2001. Maximum Security. (3rd Edn.), Sams, Indianapolis.

Avolio, F.M. and M.J. Ranum, 1994. A Network Perimeter with Secure External Access, pp: 5 http://www.alw.nih.gov/security/FIRST/paper/ firewall/isosc.

Akdeniz, Y., 1996. Cryptography and Encryption. http://www.leads.ac.uk/law/pgs/Yaman/crypto.html.

Aydos, M., 2000. Efficient Wireless Security Protocols Based on Elliptic Curve Cryptography, Ph.D Thesis. Oregon State University, pp: 132.

Bace, R., 2000. Intrusion Detection, Macmillan Publishing Co.

Barkeley, J., 1996. Security in Open systems, http://cssc.ncsl.mst.

Beker, H. and F. Piper, 1985. Securer Speech Communications. Academic Press.

Carroll, J. and L. Robbins, 1988. Computer Cryptanalysis, Technical Report No.223. Department of Computer Science, University of Western Ontario.

Coppersmith, D., 1987. Cryptography. IBM, J. Res. Dev., 31: 224-248.

Federrath, H., A. Jerichow, D. Keslogan and A. Pfitzman, 1997. Security in Public Mobile Communication Networks. Proceedings of the IFIP T6 International Workshop on Personal Wireless communications, Prague, pp: 105-116.

Forrest, S., S.A. Hofmeyr and A. Somayaji, 1997. Computer Immunology. Commun. ACM., 40: 88-96.

Herberlein, L.T., G.V. Dias, K.N. Levitt, B. Mukerejee, J. Wood and D. Wolber, 2001. A Network Security Monitor. In: Proc. IEGE. Symp. Res. Security and Privacy, pp: 296-304.

Hughes, L.J., 1995. Actually Useful Internet security Techniques. New Roders Publishing Co.

Kendall, K.E. and J.E. Kendall, 1995. Systems Analysis and Design. Prentice-Hall, Inc., New Jersey.

Leon-Garcia, G. and I. Widjaja, 2000. (Communication Networks: Fundamental Concepts and Key Architectures. McGraw-Hill.

Longley, D., W. Caelli and M. Shain, 1992. Information Security Handbook. Stockton Press, New York.

Menezes, A., P. Van Oorschot and S. Vanstone, 1997. Handbook of Applied Cryptology. CRS Press, http://www.cacr.math.uwaterloo.ca.

Milenkovic, M., 1992. Operating Systems: Concepts and design, (2nd Edn.), McGraw-Hill, Singapore.

Norton, P., 1996. Introduction to Computers, (3rd Edn.), Glencoe/McGraw-Hill, OH, USA., pp: 310.

Olorunfemi, T. and O.F. Oladipo, 2006. Security in Open Source Software: A Critical Analysis. Conf. Proc. (Itegboje, A.O. (Ed)) 8th Int. Conf. Inform. Tech. Capacity Building: The Future of Nig. Econ. Growth, 16: 277-282.

Patterson, W., 2004. An Introduction to Contemporary Information security Issues, In: Contemporary Applications of the Mathematical and Computer Sciences to Development Problems (Ed. Ekhaguere, G.O.S). International Centre for Mathematical and Computer Sciences.

Poulsen, 1999. Essentials of Microsoft Networking, Ziff-Davis Educational, New York.

Proctor, P., 2001. The Practical Intrusion Detection Handbook. Prentice-Hall.

Rabah, K., 2004. Data Security and Cryptographic Techniques-A Review. Inform. Tech. J., 3: 106-132.